UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

Deborah S. Hunt
Clerk

100 EAST FIFTH STREET, ROOM 540
POTTER STEWART U.S. COURTHOUSE
CINCINNATI, OHIO 45202-3988

Tel. (513) 564-7000
www.ca6.uscourts.gov

Filed: November 09, 2021

Mr. David Lawrence Doughten
4403 St. Clair Avenue
Cleveland, OH 44103

Ms. Laura McMullen Ford
Office of the U.S. Attorney
801 W. Superior Avenue
Suite 400
Cleveland, OH 44113

Ms. Catherine Adinaro Shusky
Federal Public Defender's Office
1660 W. Second Street
Suite 750
Cleveland, OH 44113

Re: Case Nos. 19-4247/19-4273, *USA v. Bogdan Nicolescu*
Originating Case No. : 1:16-cr-00224

Dear Counsel,

The court today released an amended opinion in the above cases.

Enclosed is a copy of the court's amended opinion together with the amended judgment which has been entered in conformity with Rule 36, Federal Rules of Appellate Procedure.

Yours very truly,

Deborah S. Hunt, Clerk

Cathryn Lovely
Deputy Clerk

GOVERNMENT EXHIBIT
C

cc: Ms. Sandy Opacich

Enclosures

Mandate to issue.

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

Nos. 19-4247/4273

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

v.

BOGDAN NICOLESCU (19-4247); RADU MICLAUS (19-4273),

Defendants - Appellants.

FILED
Nov 09, 2021
DEBORAH S. HUNT, Clerk

Before: WHITE, LARSEN, and NALBANDIAN, Circuit Judges.

AMENDED JUDGMENT

On Appeal from the United States District Court
for the Northern District of Ohio at Cleveland.

THIS CAUSE was heard on the record from the district court and was argued by counsel.

IN CONSIDERATION THEREOF, it is ORDERED that Bogdan Nicolescu's and Radu Miclaus's convictions are AFFIRMED, their sentences are VACATED, and the cases are REMANDED to the district court for resentencing consistent with the majority opinion of this court.

ENTERED BY ORDER OF THE COURT

Deborah S. Hunt, Clerk

RECOMMENDED FOR PUBLICATION
Pursuant to Sixth Circuit I.O.P. 32.1(b)

File Name: 21a0257p.06

UNITED STATES COURT OF APPEALS

FOR THE SIXTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

BOGDAN NICOLESCU (19-4247); RADU MICLAUS (19-4273),

Defendants-Appellants.

Nos. 19-4247/4273

Appeal from the United States District Court for the Northern District of Ohio at Cleveland.
No. 1:16-cr-00224—Patricia A. Gaughan, District Judge.

Argued: March 3, 2021

Decided and Filed: November 9, 2021

Before: WHITE, LARSEN, and NALBANDIAN, Circuit Judges.

COUNSEL

ARGUED: David L. Doughten, Cleveland, Ohio, for Appellant in 19-4247. Catherine Adinaro Shusky, OFFICE OF THE FEDERAL PUBLIC DEFENDER, Cleveland, Ohio, for Appellant in 19-4273. Laura McMullen Ford, UNITED STATES ATTORNEY'S OFFICE, Cleveland, Ohio, for Appellee. **ON BRIEF:** David L. Doughten, Cleveland, Ohio, for Appellant in 19-4247. Catherine Adinaro Shusky, OFFICE OF THE FEDERAL PUBLIC DEFENDER, Cleveland, Ohio, for Appellant in 19-4273. Laura McMullen Ford, UNITED STATES ATTORNEY'S OFFICE, Cleveland, Ohio, for Appellee.

WHITE, J., announced the judgment and delivered the opinion of the court in which she joined in all but Section III.D., and LARSEN and NALBANDIAN, JJ., joined in full. WHITE, J. (pp. 29–30), delivered a separate opinion dissenting from Part III.D. of the court's opinion.

AMENDED OPINION

HELENE N. WHITE, Circuit Judge [Except as to Section III.D.]. For nine years, Defendants-Appellants Radu Miclaus and Bogdan Nicolescu ran a sophisticated, multimillion-dollar cyber-fraud ring out of Romania. They were extradited to the United States, and a federal jury in Ohio convicted them of wire fraud, conspiracy to commit wire fraud, conspiracy to commit computer fraud, aggravated identity theft, conspiracy to commit money laundering, and conspiracy to traffic in counterfeit service marks. The district court sentenced them to eighteen and twenty years' imprisonment, respectively. On appeal, they raise several challenges to their convictions and sentences. We **AFFIRM** their convictions, **VACATE** their sentences, and **REMAND** for resentencing.

I.

Beginning around 2007, Nicolescu, Miclaus, and a handful of coconspirators began posting fake car auctions on eBay. Their group, dubbed "Bayrob" by the FBI (a combination of "eBay" and "robbery"), set up auctions that appeared to show vehicles for sale by US-based sellers. In reality, Bayrob had neither vehicles to sell nor a US address. Operating from in and around Bucharest, Romania, the group used various technologies to conceal its IP addresses, and employed US-based "money mules," (falsely described to victims as "eBay Escrow Agents") to collect payments from unsuspecting buyers. The money mules then wired the victims' payments to various locations in Europe, where individuals associated with Bayrob collected the payments and brought them to Miclaus and Nicolescu in Romania. All told, the Bayrob group orchestrated the eBay fraud more than 1,000 times and reaped between $3.5 million and $4.5 million.

At some point in 2014, Bayrob began employing a custom-made trojan horse virus to facilitate new money-making schemes. Nicolescu, a skilled computer programmer, created the virus, which he embedded in links in the group's eBay auctions and in spam emails widely disseminated by Bayrob. Once a victim clicked the link and downloaded the virus onto the victim's computer, it ran quietly in the background until the unsuspecting victim tried to visit

certain popular websites, including eBay, Facebook, PayPal, Gmail, Yahoo, and Walmart. At that point, instead of connecting to the real website, the virus discreetly redirected the victim's computer to a look-a-likewebsite created by Bayrob, which collected the victim's account credentials, identities, and credit-card information, and stored it all on Bayrob's servers in Romania. Bayrob collected more than 70,000 account credentials this way, including 25,000 stolen credit-card numbers. Bayrob used the stolen credit cards to pay its own expenses, including costs for server space, VPNs, and registering domain names, and it sold some of the stolen credit cards on AlphaBay, a website on the dark web frequented by criminals, for prices ranging from $1–$35.

Around the same time, Bayrob concocted a third money-making scheme. This time it harnessed the processing power of its network of 33,000 virus-infected computers to "mine" for cryptocurrency. Nicolescu's trojan horse virus worked by commandeering an infected computer's processor and forcing it to solve difficult mathematical equations that generate bitcoin, a process known as "cryptomining." With their computers' processing power tied up generating bitcoin for Bayrob, the victims' computers slowed to a crawl. Bayrob exchanged the bitcoins generated by its cryptomining activities for cash, generating approximately $10,000–$20,000 per month in 2014, and $30,000–$40,000 per month in 2015 and 2016.

The FBI caught on to Bayrob's activities in 2015 and executed a search warrant on the cell phone of Tiberiu Danet, a Bayrob member, as he traveled through the Miami airport. Using information obtained from Tiberiu's phone, the FBI and Romanian police executed a search warrant on Nicolescu's, Miclaus's, and Tiberiu's residences in Romania. The searches turned up a trove of servers, hard drives, and other computing equipment used by the group. The FBI was not able to decrypt much of the information on Bayrob's servers, but the cache of seized files the FBI was able to review included spreadsheets the group used to keep track of its victims and spreadsheets showing money Bayrob had moving through its money-mule network in the United States and Europe.

In 2016, Nicolescu and Miclaus were indicted for conspiracy to commit wire fraud, twelve counts of wire fraud, conspiracy to commit computer fraud, conspiracy to traffic in

counterfeit service marks, five counts of aggravated identity theft, and conspiracy to commit money laundering. They were convicted on all counts after a two-and-a-half-week jury trial.[1]

At Defendants' sentencing hearing, FBI agent Ryan MacFarlane testified that the eBay scheme generated between $3.5 million and $4.5 million in losses. The FBI calculated that figure by reviewing spreadsheets Bayrob used to keep track of its victims and cross-referencing the information in the spreadsheets with victim complaints filed with the FBI's Internet Crime Complaint Center (ICCC). MacFarlane estimated that the true eBay loss figure was substantially higher than $3.5 to $4.5 million, since only 30–35% of victims filed complaints with the ICCC. According to MacFarlane, true losses may have been as high as $10 million to $30 million.

At the conclusion of the sentencing hearing, the district court calculated Nicolescu's and Miclaus's Guidelines range for the conspiracy-to-commit-money-laundering grouping (Counts 1–15 and 21). The district court added eighteen levels to their Guidelines calculation under U.S.S.G. § 2B1.1(b)(1)(J) for causing a loss between $3.5 and $9.5 million, two levels under U.S.S.G. § 2B1.1(b)(4) for being in the business of receiving and selling stolen property, two levels under U.S.S.G. § 2B1.1(b)(11)(B)(i) for trafficking unauthorized access devices, four levels under U.S.S.G. § 2B1.1(b)(19)(A)(ii) for having been convicted of an offense under 18 U.S.C. § 1030(a)(5)(A), and four levels under U.S.S.G. § 3B1.1(a) for being an organizer or leader of criminal activity, as well as other enhancements not at issue in this appeal. The result was an adjusted offense level of forty-three, which at criminal history category I produced a Guidelines range of life imprisonment. Since a life sentence exceeded the statutory twenty-year maximum on any of the offenses in the grouping, the parties agreed to (and the district court applied) a five-level reduction for an applied total offense level of thirty-eight. After the five-level reduction, Nicolescu's and Miclaus's Guidelines range was 235 to 293 months. They were sentenced to 216 and 192 months' imprisonment, respectively, on Counts 1 through 13 and 21, concurrent sentences of sixty months on Count 14 and 120 months on Count 15, and mandatory twenty-four month sentences on Counts 16 through 20, to run concurrently with each

[1]The jury acquitted Nicolescu and Miclaus on sentencing enhancements under 18 U.S.C. § 3559(g)(1) for false registration of domain names (pertaining to all counts).

other but consecutively to all the other sentences, for a total sentence of 240 (Nicolescu) and 216 (Miclaus) months' imprisonment.

This appeal followed.

II.

Nicolescu and Miclaus each appeal one substantive count of conviction and the application of multiple sentencing enhancements. We consider the challenges to their substantive convictions first.

A.

Nicolescu contends the district court erred in denying his motion for acquittal based on insufficiency of the evidence on Count 14, which charges conspiracy to violate 18 U.S.C. § 1030(a)(5)(A) and two other statutes.

We review a district court's denial of a motion for judgment of acquittal *de novo*. *United States v. Howard*, 947 F.3d 936, 947 (6th Cir. 2020). When reviewing the sufficiency of the evidence, we assess "whether, after viewing the evidence in the light most favorable to the prosecution, *any* rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *Jackson v. Virginia*, 443 U.S. 307, 319 (1979).

The jury convicted Nicolescu and Miclaus on Count 14, which alleged a conspiracy with three objects:

> (i) to intentionally access a computer without authorization, and thereby obtain information from a protected computer, and the offense was committed for purposes of commercial advantage and private financial gain, in violation of Title 18, United States Code, Section 1030(a)(2)(C); and
>
> (ii) to intentionally access a computer without authorization and by means of such conduct furthered the intended fraud and obtained something of value, specifically, money, in excess of 3 to 4 million dollars, in violation of Title 18, United States Code, Section 1030(a)(4); and
>
> (iii) to knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, and the offense caused damage affecting

> ten or more protected computers in a one year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B).

R. 1, PID. 24 (Indictment ¶ 89). On appeal, Nicolescu challenges the sufficiency of the evidence on only the third object of the conspiracy, § 1030(a)(5)(A) and (c)(4)(B). Since this court must assume the evidence on the two unchallenged objects was sufficient, his failure to challenge the sufficiency of the evidence on the other two charged objects is fatal to his claim. *See Griffin v. United States*, 502 U.S. 46, 56–57 (1991) ("[W]hen a jury returns a guilty verdict on an indictment charging several acts in the conjunctive . . . the verdict stands if the evidence is sufficient with respect to any one of the acts charged." (alteration in original) (quoting *Turner v. United States*, 396 U.S. 398, 420 (1970))). Moreover, the jury heard testimony from multiple witnesses that Nicolescu's computer virus caused its victims' computers to run slowly because the virus was using their computers' processing power to mine for bitcoin. Such testimony was enough for a reasonable juror to find that Nicolescu conspired to damage a protected computer, in violation of § 1030(a)(5)(A) and (c)(4)(B).[2]

B.

Miclaus contends the district court erred in denying his motion for acquittal on Counts 16 through 20, which charged aggravated identity theft in violation of 18 U.S.C. § 1028A, because

---

[2]Nicolescu's brief describes his challenge as one to the sufficiency of the evidence, *see* Nicolescu Br. at 43 ("The evidence is insufficient to establish that the appellant conspired to violate 18 U.S.C. §1030(a)(5)(A)"), but to the extent Nicolescu intended to argue—as some of his briefing seems to suggest—that "slowing" of a computer cannot constitute "damage" to a computer as a matter of law, *see id.* ("Here, Nicolescu challenges whether he caused damage as required by the statute."), this challenge too fails.

18 U.S.C. § 1030(e)(8) defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information[.]" Applying the same statute in the civil context, we looked to the ordinary meaning of the terms "impairment," "integrity," and "availability" and defined "damage" for purposes of § 1030(a)(5)(A) as "a transmission that weakens a sound computer system—or, similarly, one that diminishes a plaintiff's ability to use data or a system[.]" *Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am.*, 648 F.3d 295, 301 (6th Cir. 2011). Nicolescu's virus, which caused infected computers to "run very slowly," R. 233, PID. 3729, would constitute an "impairment to the integrity . . . of . . . [the] system." *See* 18 U.S.C. § 1030(e)(8). In other words, the virus was a "transmission that . . . diminishe[d] a [victim's] ability to use . . . a system." *Pulte Homes, Inc.*, 648 F.3d at 301; *see also United States v. Carlson*, 209 F. App'x 181, 184–85 (3d Cir. 2006) (finding that criminal defendant intentionally caused "damage" to victim's computer under § 1030(a)(5)(A) when he flooded victim inboxes with thousands of spam emails, "which would clog the address, result in delays, and at times require the purging of all e-mails, causing valuable business-related e-mails to be permanently lost").

the government did not present evidence that Miclaus aided and abetted the "use" of each of the five aggravated-identity-theft victims' credit cards. Miclaus Br. at 43–50.

We review the district court's denial of Miclaus's motion for judgment of acquittal *de novo*, and again assess whether, viewing the evidence in the light most favorable to the prosecution, any rational juror could have found the essential elements proven beyond a reasonable doubt. *Howard*, 947 F.3d at 947.

To sustain a conviction for aggravated identity theft, the government must prove the defendant "(1) knowingly used, without lawful authority, a means of identification of another person; and (2) used that means of identification during and in relation to an enumerated predicate felony." *United States v. Vance*, 956 F.3d 846, 857 (6th Cir.), *cert. denied*, 140 S. Ct. 2819 (2020). Here, the alleged predicate felonies were computer fraud under § 1030 and wire fraud under § 1343. The jury was instructed, pursuant to Sixth Circuit Pattern Jury Instruction 15.04, that "use" means "active employment of the means of identification during and in relation to the [predicate felony]. Active employment includes activity such as displaying or bartering. 'Use' also includes a person's reference to a means of identification in his possession for the purpose of helping to commit the [predicate felony]." R. 242, PID. 5759–60. Miclaus does not argue that a credit-card number is not a "means of identification," nor does he challenge our pattern jury instruction's definition of "use," so we assume the correctness of both here.

At trial, the jury heard that the names, addresses, and credit-card numbers of the five victims identified in Counts 16 through 20 were found on one of Bayrob's internal victim-tracking spreadsheets (Exhibit 1204 at trial). An FBI agent testified that the FBI spoke with four of the victims and the fifth victim's wife and confirmed that the identity and credit-card information in Bayrob's spreadsheet was accurate. Some of the victims testified at trial and confirmed the same. Valentin Dima, a Bayrob member who cooperated with the government, testified that Bayrob had a practice of testing the validity of each credit-card number before adding it to its victim-tracking spreadsheets by "creating e-mail addresses through Yahoo, and then . . . upgrad[ing] the account [to] Yahoo plus," which required a valid credit card, to see if each stolen credit card was still valid. R. 240, PID. 5341–42. The spreadsheet contained a column with "0's" and "1's" for each card, with "1" indicating that the card was still valid and

could be used for purchases, and "0" indicating that the card did not work. The spreadsheet contained another column where Bayrob members noted operational purchases they made with the stolen cards, including for website hosting and VPNs.

Miclaus contends the government failed to prove Bayrob "used" each victim's credit-card number because not every victim testified that fraudulent purchases were made on their credit cards. Miclaus's challenge fails because even if fraudulent purchases were not made on each card, Dima testified that his job was to test each credit card before adding it to the spreadsheet, and the jury could see that the spreadsheet contained "0's" and "1's" for each card.[3] A means of identification is "used" whenever it is "employ[ed]" or "convert[ed] to one's service." *United States v. Michael*, 882 F.3d 624, 626 (6th Cir. 2018) (quoting Webster's New International Dictionary 2806 (2d ed. 1942)). Sending a stolen credit-card number to Yahoo as part of a sham email account upgrade transaction for the sole purpose of having Yahoo run that credit-card number and report back whether it is still valid for future operational purchases is an "active employment" of that stolen credit-card number. Indeed, situations where a defendant impersonates a victim—as Bayrob did when it purported to be each of the victims in transactions with Yahoo—were the "principal target" of § 1028A. *Michael*, 882 F.3d at 627. Accordingly, when viewed in the light most favorable to the government, the evidence was sufficient for a reasonable juror to find Miclaus guilty on Counts 16 through 20.

C.

Miclaus also challenges the substance of the district court's aggravated-identity-theft jury instruction. He contends that it omitted an element: that Miclaus be found to have committed an enumerated felony.

Miclaus did not object to the instruction at trial, so we review for plain error. *United States v. Small*, 988 F.3d 241, 254 (6th Cir. 2021). "In the context of challenges to jury

[3]Even if Dima did not specifically testify that he tested each of the five aggravated-identity-theft victims' credit-card numbers, Dima's testimony about his activities testing cards, coupled with the evidence that the spreadsheet contained either a "0" or a "1" for every card, is circumstantial evidence that the five aggravated-identity-theft victims' credit-card numbers were tested. "Circumstantial evidence alone is sufficient to sustain a conviction and such evidence need not remove every reasonable hypothesis except that of guilt." *Howard*, 947 F.3d at 947 (quoting *United States v. Lowe*, 795 F.3d 519, 522–23 (6th Cir. 2015)).

instructions, plain error requires a finding that, taken as a whole, the jury instructions were so clearly erroneous as to likely produce a grave miscarriage of justice." *Id.* (quoting *United States v. Newsom*, 452 F.3d 593, 605 (6th Cir. 2006)).

As noted in the preceding section, to sustain a conviction for aggravated identity theft, the government must prove the defendant "(1) knowingly used, without lawful authority, a means of identification of another person; and (2) used that means of identification during and in relation to an enumerated predicate felony." *Vance*, 956 F.3d at 857. Here, the indictment alleged the predicate felonies were "Computer Fraud" under § 1030, and "Wire Fraud" under 18 U.S.C. § 1343, which are predicate felonies under § 1028A. *See* § 1028A(c)(4) (predicate offenses include provisions in chapter 47, which includes § 1030 computer fraud); § 1028A(c)(5) (predicate offenses include provisions in chapter 63, which includes § 1343 wire fraud). Paragraph 123 of the indictment alleges:

> 123. From on or about February 25, 2013, through on or about July 1, 2015, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendants BOGDAN NICOLESCU, TIBERIU DANET, and RADU MICLAUS, and others presently known and unknown to the Grand Jury, did knowingly use, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), to wit, the commission of Computer Fraud, a violation of Title 18, United States Code, Section 1030, and Wire Fraud, a violation of Title 18, United States Code, Section 1343, knowing that the means of identification belonged to another actual person, in violation of Title 18, United States Code, Sections 1028A(a)(l) and 2.

R. 1, PID 34 (Indictment ¶ 123). At trial, the district court's jury instruction on the aggravated-identity-theft count read:

> Counts 16 through 20 of the indictment charge Defendants Bogdan Nicolescu and Radu Miclaus with the crime of aggravated identity theft, Title 18 United States Code, Sections 1028A(a)(1) and 2.
>
> Count 16 through 20 of the indictment charge each Defendant with using a means of identification of another person during and in relation to a felony violation listed in the statute.
>
> For you to find each Defendant guilty of this crime, you must find that the Government has proved each and every one of the following elements beyond a reasonable doubt.

> First, that each Defendant committed the following violation charged in Count 16 through 20. The violation charged in Count 16 through 20 is a felony violation listed in the statute;
>
> Second, that each Defendant knowingly used a means of identification of another person without lawful authority;
>
> Third, that each Defendant knew the means of identification belonged to another person;
>
> Fourth, that the use was during and in relation to the crime charged in Counts 16 through 20;
>
> . . .
>
> The term "during and in relation to" requires that the means of identification have some purpose or effect with respect to the crime charged in Counts 16 through 20. In other words, the means of identification must facilitate or further or have the potential of facilitating or furthering the crime charged in Counts 16 through 20, and its presence or involvement cannot be the result of accident or coincidence.

R. 242, PID. 5758–61.

Miclaus is correct that the district court's aggravated-identity-theft jury instruction was erroneous. The instruction should have specified, when describing the first and fourth elements and defining the term "during and in relation to," that the predicate felonies charged in Counts 16 through 20 were § 1343 wire fraud and § 1030 computer fraud. Instead, the instruction referred back to Counts 16 to 20 as a whole. Such an error does not automatically warrant reversal, however. *See United States v. Kuehne*, 547 F.3d 667, 682 (6th Cir. 2008) (failure to instruct jury on elements of predicate offense in 18 U.S.C. § 924(c)(1) conviction was harmless because "the jury was presented with uncontroverted evidence supporting the predicate drug offenses"). Indeed, in the context of this case, we find it highly unlikely that the district court's error led any juror astray.

To start, the jury had the indictment during its deliberations and the indictment clearly explains that the predicate offenses are § 1030 computer fraud and § 1343 wire fraud. The jury was instructed on the substantive elements of § 1030 computer fraud when it was instructed on Count 14, which charged conspiracy to commit computer fraud, and on the substantive elements of wire fraud when it was instructed on Counts 2 through 13, which charged wire fraud.

It convicted Nicolescu and Miclaus on all twenty-one counts, including wire fraud and conspiracy to commit computer fraud.

Further, the aggravated-identity-theft allegations were inextricably intertwined with the computer-fraud and wire-fraud allegations. Over the course of the two-week trial, the jury heard testimony from some of the aggravated-identity-theft victims that their computers became infected with a virus after visiting an eBay auction, and it heard from the FBI that the aggravated-identity-theft victims' credit-card information was found in Bayrob's internal spreadsheets. That created the strong inference that Nicolescu and Miclaus obtained the victims' credit-card information via the virus, and the jury was presented with no alternative explanation for how the aggravated-identity-theft victims' credit-card information ended up in Bayrob's spreadsheets. The jury then heard that Bayrob tested the stolen credit cards in preparation for—and in some cases to actually make—operational purchases necessary to support its vast online operation. This all adds up to a strong circumstantial case for aggravated identity theft: Bayrob came into possession of the aggravated-identity-theft victims' credit-card information using the fake eBay auctions and the virus, which violated § 1343 and § 1030, and they used the stolen credit-card information when they verified the cards and made operational purchases with them, in violation of § 1028A. Because the offenses were so intertwined, it is unlikely that any juror could have believed that Miclaus was guilty of aggravated identity theft *without* also believing he was guilty of computer and wire fraud. We therefore find it unlikely that the district court's error "produce[d] a grave miscarriage of justice" here. *Newsom*, 452 F.3d at 605. Miclaus's claim is without merit.

III.

Nicolescu and Miclaus also challenge multiple sentencing enhancements applied by the district court. We consider each in turn.

A.

The district court applied an eighteen-level Guidelines enhancement under U.S.S.G. § 2B1.1(b)(1)(J) for causing losses of more than $3.5 million and less than $9.5 million. Nicolescu contends that was error because the government's evidence only established a

$1.1 million gain for Bayrob as a result of the eBay scheme and $100,000 in fraudulent purchases on victims' credit cards. Nicolescu argues that though a loss calculation under § 2B1.1(b)(1)(J) may include intended losses in addition to proven losses, doing so in this case rendered the district court's loss calculation unduly speculative, since the government did not provide wire transfer information for all $3.5 million in alleged losses and instead relied on a $500-per-stolen-credit-card multiplier found in the Guidelines commentary to reach the estimated loss figure. Nicolescu contends that the government should have been required to present evidence of the credit limit of each of the stolen credit cards.

Under the Guidelines, if the loss attributable to a theft exceeds $3.5 million but is less than $9.5 million, the district court is instructed to increase the offense level by eighteen levels. § 2B1.1(b)(1)(J). Section 2B1.1's application notes define the applicable loss amount as "the greater of actual loss or intended loss." *Id.* § 2B1.1 cmt. n.3(A). "Actual loss" is "the reasonably foreseeable pecuniary harm that resulted from the offense." *Id.* § 2B1.1 cmt. n.3(A)(i). "Intended loss" is "the pecuniary harm that the defendant purposely sought to inflict[,]" which may include losses "that would have been impossible or unlikely to occur[.]" *Id.* § 2B1.1 cmt. n.3(A)(ii). In calculating the loss amount, the district court "need only make a reasonable estimate of the loss," and its determinations are "entitled to appropriate deference." *Id.* § 2B1.1 cmt. n.3(C). If the loss amount cannot reasonably be determined, the district court may use "the gain that resulted from the offense as an alternative measure[.]" *Id.* § 2B1.1 cmt. n.3(B).

As a threshold matter, the district court cited both Agent MacFarlane's testimony regarding the eBay-auction scheme and the credit cards Bayrob sold on AlphaBay when addressing the $3.5 million loss figure, but the district court found that "Agent Mac[F]arlane's testimony [about the losses attributable to the eBay scheme] alone satisfies the Government's burden." R. 230, PID. 3257. Therefore, even if this court's recent decision in *United States v. Riccardi* renders invalid any loss calculation based on a $500-per-stolen-credit-card multiplier, we need not address the stolen credit cards Bayrob sold on AlphaBay if the losses from the eBay scheme —which do not rely on a multiplier—totaled more than $3.5 million. *See* 989 F.3d 476, 489 (6th Cir. 2021) (invalidating § 2B1.1 cmt. n.3(F)(i)'s $500-per-access-device multiplier).

We review the district court's findings regarding the losses attributable to the eBay scheme under a deferential clear-error standard. *Id.* at 487. In arriving at the $3.5 million loss figure, the district court relied heavily on Agent MacFarlane's testimony at the sentencing hearing that the eBay scheme generated losses between $3.5 million and $4.5 million. The FBI calculated that figure after reviewing victim information found in an unencrypted spreadsheet that Bayrob members used to track payments from their victims, and then cross-referencing that information with complaints in the FBI's ICCC database and tallying the loss amounts from those complaints. The FBI was able to match the information found on Bayrob's servers with particular victim complaints by looking at "specific indicators that were associated with the Bayrob Group, such as known e-mail accounts, known money mules, known fax numbers and other technical indicators that allowed [the FBI] to identify complaints that were related to the Bayrob Group[.]" R. 230, PID. 3201. According to MacFarlane, the $3.5 million figure is based only on "actual observed transactions" from ICCC "complaints that [the FBI was] able to identify" that were also "consistent with the behavior of the Bayrob eBay fraud operation." *Id.* at 3201–03. The FBI discounted ICCC complaints that alleged loss amounts that "weren't realistic." *Id.* at 3202. And, according to MacFarlane, the $3.5 million figure is a "conservative estimate" because only 30–35% of the eBay victims the FBI identified on Bayrob's servers also filed complaints with the ICCC. *Id.* at 3203–04. The FBI estimates that the actual losses from the eBay scheme may have been as high as $30 million.

"In challenging the court's loss calculation, [Nicolescu] must carry the heavy burden of persuading this Court that the evaluation of the loss was not only inaccurate, but was outside the realm of permissible computations." *United States v. Jackson*, 25 F.3d 327, 330 (6th Cir. 1994). Nicolescu's primary argument is that the district court should have used traceable gains: here the $1.1 million in wire transfers the FBI was able to trace through one of Bayrob's money mules back to Europe, instead of the $3.5 million figure provided by the FBI, which was based on verified ICCC victim complaints, but was not always backed up by evidence of specific wire transfers showing how each victim's money ended up in Bayrob's possession. The FBI was not able to trace more victim wire transfers back to Bayrob because the FBI was not able to decrypt much of the information on Bayrob's servers, and MacFarlane testified that Nicolescu and Miclaus declined to assist the FBI in identifying the other money mules the group used.

Although more specificity about Bayrob's illicit gains may have been preferable, "the district court need only make a reasonable estimate of the loss using a preponderance of the evidence standard." *United States v. Ellis*, 938 F.3d 757, 760 (6th Cir. 2019) (quoting *United States v. Wendlandt*, 714 F.3d 388, 393 (6th Cir. 2013)). And the Guidelines commentary provides that the district court "shall use the gain that resulted from the offense as an alternative measure of loss *only if* there is a loss but it reasonably cannot be determined." § 2B1.1 cmt. n.3(B) (emphasis added). Here, the district court based its $3.5 million loss calculation on (i) Agent MacFarlane's detailed testimony about the FBI's efforts to identify specific victim complaints attributable to Bayrob, including his assurances that the $3.5 million loss figure was based on "actual observed transactions," (ii) the district court's own review of Bayrob's internal victim-tracking spreadsheets, and (iii) victim statements submitted to the district court. R. 230, PID. 3258. Given the practical difficulties the government and the district court faced in obtaining more precise detail about victim losses—some of which can be attributed to Defendants' decision to encrypt the files on their servers and their refusal to provide the FBI with the decryption key—the district court's reliance on victim statements and ICCC complaints was reasonable, and we cannot say on the record before us that the district court's $3.5 million loss calculation was clearly erroneous.

B.

U.S.S.G. § 2B1.1(b)(4) provides for a two-level increase if "the offense involved receiving stolen property, and the defendant was a person in the business of receiving and selling stolen property[.]" At the sentencing hearing, the district court applied the two-level § 2B1.1(b)(4) enhancement because it found that Nicolescu and Miclaus "operated a long-standing and highly sophisticated scheme" whereby they "obtained vast amounts of credit card data, which [they] did, in fact, sell" on AlphaBay "even if [they were] not initially in the business of buying and selling property." R. 230, PID. 3263–64.

Nicolescu and Miclaus contend that was error because § 2B1.1(b)(4) was intended to apply to defendants who "fence" stolen goods for others, and Bayrob was not a fence: it only sold credit cards on the dark web that the group itself stole. Nicolescu Br. at 30; Miclaus Br. at 18. The government's brief takes a broader view of the reach of the Guideline: the government

contends that § 2B1.1(b)(4) is not limited to fencing cases, and the language of § 2B1.1(b)(4) covers situations where defendants "receive" stolen goods from a computer virus and then sell them on the dark web. Appellee's Br. at 44–45. Additionally, the government suggests that the enhancement can apply when a defendant "receives" stolen property from a coconspirator and then sells it—even when the object of the conspiracy was to steal the same property.

"When reviewing the district court's application of the Sentencing Guidelines, we review the district court's factual findings for clear error and mixed questions of law and fact *de novo*." *United States v. Tolbert*, 668 F.3d 798, 800 (6th Cir. 2012) (quoting *United States v. May*, 568 F.3d 597, 604 (6th Cir. 2009)). We review the district court's interpretation of the Sentencing Guidelines *de novo*. *Id.*

By its terms, § 2B1.1(b)(4) applies "[i]f the offense involved receiving stolen property" and "the defendant" was "in the business of receiving and selling stolen property[.]" In determining whether a defendant is "in the business of" receiving and selling stolen property, Application Note 5 to § 2B1.1 instructs courts to consider "(A) [t]he regularity and sophistication of the defendant's activities; (B) [t]he value and size of the inventory of stolen property maintained by the defendant; (C) [t]he extent to which the defendant's activities encouraged or facilitated other crimes; [and] (D) [t]he defendant's past activities involving stolen property." § 2B1.1 cmt. n.5.

We have not yet addressed whether § 2B1.1(b)(4) is limited in its application to defendants who sell goods that others have stolen, as opposed to defendants who sell goods they have stolen themselves, but in *United States v. Warshawsky*, we addressed a prior version of the same Guideline and explained that "[a] person 'in the business of receiving and selling stolen property' is a person once referred to less flatteringly as a 'fence.'" 20 F.3d 204, 214 (6th Cir. 1994). A few months later, citing *Warshawsky*, we recognized that for purposes of the enhancement, there is a difference between "a person who receives stolen property" and a person "who sells property that he himself has stolen[,]" because the Sentencing Commission "decided that fences deserve longer sentences than mere thieves" because fencing facilitates and encourages other crimes while mere thievery does not. *United States v. Koehler*, 24 F.3d 867,

871 (6th Cir. 1994). Accordingly, we explained that only those who sell goods that others have stolen are subject to the "fencing" enhancement. *Id.*

Warshawsky and *Koehler* interpreted U.S.S.G. § 2B1.2, which was deleted and consolidated with § 2B1.1 in November 1993. *United States v. Vigil*, 644 F.3d 1114, 1119 (10th Cir. 2011). The 1993 amendment also added the first clause to the current iteration of the enhancement, which now requires that "the offense involved receiving stolen property[.]" *Id.* But neither the addition of the first clause nor consolidation with § 2B1.1 provides us with reason to question what we said in *Warshawsky* and *Koehler*: the defendant must "receive" stolen goods before he can be "in the business of receiving and selling stolen property." A defendant does not "receive" goods he himself stole. *See United States v. McMinn*, 103 F.3d 216, 219 (1st Cir. 1997) ("Under the common-law tradition, stealing property from another normally does not equate with 'receiving' property from its rightful owner."); *Baugh v. United States*, 540 F.2d 1245, 1246 (4th Cir. 1976) ("[L]ogic . . . instructs us that there is an inherent inconsistency in treating a taking as a receipt."). Accordingly, § 2B1.1(b)(4) is limited in its application to professional fences—it does not apply to thieves who merely sell goods they stole.[4] Our sister circuits have almost unanimously reached the same conclusion. *See, e.g.*, *United States v. Borders*, 829 F.3d 558, 568 (8th Cir. 2016); *Vigil*, 644 F.3d at 1118; *United States v. Bradley*, 644 F.3d 1213, 1287 (11th Cir. 2011); *Kimbrew*, 406 F.3d at 1152; *McMinn*, 103 F.3d at 219–21; *United States v. Sutton*, 77 F.3d 91, 94 (5th Cir. 1996); *United States v. Braslawsky*, 913 F.2d 466, 468 (7th Cir. 1990) (coming to same conclusion about prior version of the enhancement, § 2B1.2(b)(3)(A)). *But see United States v. Collins*, 104 F.3d 143, 144 (8th Cir. 1997) (holding that a thief was "in the business" of receiving and selling stolen property when he delivered goods he had stolen to an auction house and split the proceeds with the auction house after the goods were sold).

[4]In 2001, the Sentencing Commission added Application Note 5 to § 2B1.1, which adopted a "totality of the circumstances" test for determining whether a defendant's fencing activities were frequent enough to consider him "in the business of" receiving and selling stolen property. *Vigil*, 644 F.3d at 1120. Application Note 5 had the effect of abrogating a different test this court had adopted in *Warshawsky*. *Id.* But the addition of Application Note 5 and the abrogation of the test adopted in *Warshawsky* does not affect our analysis here, since "both tests operate on the predicate that the defendant is a fence." *United States v. Kimbrew*, 406 F.3d 1149, 1154 (9th Cir. 2005).

Nonetheless, that holding does not end our inquiry here. In its brief, the government contends that Nicolescu and Miclaus are eligible for the enhancement because they "received" stolen credit cards from the computer virus Nicolescu created and Miclaus injected into his fake eBay auction listings. Appellee's Br. at 39–40. The government cites no authority in support of its novel theory of receipt. We find the government's theory to be linguistically untenable. The virus was a tool created and employed by Nicolescu and Miclaus to steal victims' credit-card numbers. Tools and other inanimate objects do not commit larceny. People do. For that reason, Defendants cannot "receive" stolen goods from their tools. Were we to adopt the government's reading, it would effectively collapse larceny and receipt of stolen goods—"distinct substantive offense[s]" at common law—into the same offense. 76 C.J.S. Receiving Stolen Goods § 1 (2021); *see also McMinn*, 103 F.3d at 219. We decline to adopt such an anomalous interpretation.

Moreover, our interpretation is consistent with the Application Note, which we are bound to apply. *See Stinson v. United States*, 508 U.S. 36, 38 (1993); *United States v. Paauwe*, 968 F.3d 614, 618 (6th Cir. 2020). Application Note 5 to § 2B1.1 instructs courts to consider "[t]he extent to which the defendant's activities encouraged or facilitated other crimes" when deciding whether to apply the enhancement. Fences induce others to commit property crimes by providing them with a ready market for their stolen goods. *See Warshawsky*, 20 F.3d at 215; *Koehler*, 24 F.3d at 871. Thieves who sell goods they stole typically do not. Here, the government conceded at oral argument that there was no evidence that Bayrob sold goods stolen by anyone outside of the group. Thus, there is no evidence that Nicolescu and Miclaus acted as "fences."

Alternatively, the government suggests that Nicolescu and Miclaus are subject to this enhancement because the individuals within Bayrob responsible for stealing some of the credit cards were not necessarily the same people who sold them on AlphaBay. Appellee's Br. at 41 ("Nicolescu gave Valentin Danet access to Bayrob's Alpha Bay account to sell the stolen credit cards and provided the bitcoin payment wallets used for the sales."); *Id.* at 45 ("[T]he defendant[s] received some of the stolen data in part through phishing-initiated theft that was developed by a co-conspirator."); Oral Arg. at 28:50 (arguing that Nicolescu and Miclaus

received stolen cards from other Bayrob members who had personally stolen them). In other words, the government's argument is that an individual who "receives" stolen property *from a coconspirator* and then sells it is operating as a fence. The government's theory is untenable where, as here, the object of the conspiracy was *to steal* the property. If two or more individuals conspire to steal something, all members of the conspiracy are accountable for the theft. *See* U.S.S.G. § 1B1.3(a)(1)(B) (outlining requirements to hold defendant liable for jointly undertaken conduct in calculating advisory Guidelines sentencing range); *United States v. Hamm*, 952 F.3d 728, 744 (6th Cir. 2020) (discussing requirements for holding a defendant liable for the crimes of a coconspirator under *Pinkerton v. United States*, 328 U.S. 640 (1946)); *see also United States v. Gilbert*, 725 F. App'x 370, 373 (6th Cir. 2018) (discussing *Pinkerton* liability in the context of aggravated identity theft). It would be strange, therefore, not to think of such conspirators as participating in the theft, even if they do not do so physically or personally.

If an individual is responsible for stealing property, then he cannot *fence* the same property. *See Koehler*, 24 F.3d at 871; *Warshawsky*, 20 F.3d at 214–15. Thus, even if other members of Bayrob completed some of the credit-card thefts themselves and then passed those cards on to Nicolescu or Miclaus to sell (or if defendants stole the cards and gave them to other Bayrob members to sell), the "seller" did not receive stolen property within the meaning of § 2B1.1(b)(4). The seller conspired to steal. That made him a thief, not a fence. *Cf. Kimbrew*, 406 F.3d at 1150–54 (declining to apply fencing enhancement where defendant conspired to obtain computers via fraud, which a coconspirator would then re-sell).

The government looks for contrary support in the Eighth Circuit's decision in *United States v. Borders*. *See* 829 F.3d at 568–69. In *Borders*, the Eighth Circuit found that it was not clear error to apply § 2B1.1(b)(4) to a defendant who "often scouted and stole trucks" for another defendant who gave him "shopping lists" of property to steal. *Id.* at 569. It also applied the enhancement to the defendant who wrote the "shopping lists" and sold the property. *Id.* But *Borders*'s § 2B1.1(b)(4) analysis did not grapple with the fact that both defendants were engaged in a conspiracy to steal the property in question. As such, we do not find it instructive.

We conclude that the district court erred in applying a two-level enhancement under § 2B1.1(b)(4) for receiving and selling stolen property.

C.

The district court applied a four-level leadership-role enhancement under U.S.S.G. § 3B1.1(a) to both Defendants' Guidelines calculations. On appeal, Nicolescu, whose online moniker was "Master Fraud 1," R. 236, PID. 4383, contends that he was, in fact, not the master of the frauds. He asserts that he "was not the leader in the money laundering" and was "equally responsible as others, but had no more authority tha[n] at least two other members of Bayrob[.]" Nicolescu Br. at 30–31. In his telling, only a two-level enhancement was warranted. Miclaus argues that the leadership-role enhancement was not warranted because he "was not recruiting members, writing code, maintaining the servers, or recruiting money mules" and "[h]is only roles were to post fraudulent auctions on eBay and to, occasionally, accept money from Antonovici to pass along to other members of the group." Miclaus Br. at 39.

This court reviews "the district court's legal conclusion that a person is an organizer or leader under [§] 3B1.1 deferentially, and its factual findings for clear error." *United States v. Sexton*, 894 F.3d 787, 794 (6th Cir. 2018) (alteration in original) (internal quotation marks omitted) (quoting *United States v. House*, 872 F.3d 748, 751 (6th Cir. 2017)). "Under the clear-error standard, we abide by the court's findings of fact unless the record leaves us with the definite and firm conviction that a mistake has been committed." *Id.* (quoting *United States v. Yancy*, 725 F.3d 596, 598 (6th Cir. 2013)). The deferential review of the district court's ultimate legal conclusion is based on the recognition that the "trial judge is most familiar with the facts and is best situated to determine whether someone is or is not a 'leader' of a conspiracy that the jury found existed." *United States v. Washington*, 715 F.3d 975, 983 (6th Cir. 2013).

Section 3B1.1(a) provides for a four-level increase "[i]f the defendant was an organizer or leader of a criminal activity that involved five or more participants or was otherwise extensive[.]" To decide whether a defendant was an "organizer or leader," the Guidelines direct courts to consider a number of factors, including

> the exercise of decision making authority, the nature of participation in the commission of the offense, the recruitment of accomplices, the claimed right to a larger share of the fruits of the crime, the degree of participation in planning or organizing the offense, the nature and scope of the illegal activity, and the degree of control and authority exercised over others.

§ 3B1.1 cmt. n.4. "The government bears the burden of proving that the enhancement applies by a preponderance of the evidence." *United States v. Vandeberg*, 201 F.3d 805, 811 (6th Cir. 2000). "A district court need not find each factor in order to warrant an enhancement." *United States v. Castilla–Lugo*, 699 F.3d 454, 460 (6th Cir. 2012).

Nicolescu. At the sentencing hearing, the district court explained that "[w]itnesses testified that [Nicolescu] was the mastermind behind the entire operation" which "includes the money laundering scheme." R. 230, PID. 3275–76. The district court noted that Nicolescu was "a constant member of the scheme," and found that he was a leader in the conspiracy because he "controlled the money mule network in the United States which was necessary to the success of the money laundering scheme" and "provided directives to other members in the conspiracy." *Id.*

Ample evidence supported a finding that Nicolescu was the primary leader of the Bayrob group and the orchestrator of its various schemes, including the money-laundering conspiracy. Over the course of the two-and-a-half-week trial, the court heard how Nicolescu created the computer virus, recruited the money mules, instructed the mules to divide the wire transfers into increments below $3,000 to avoid detection, and kept 25% of the profits—the highest percentage (along with two other members) in the Bayrob group. The district court did not err in applying a four-level enhancement to Nicolescu's Guidelines calculation under § 3B1.1(a).

Miclaus. The government argued that a four-level enhancement was warranted for Miclaus because he was one of only two Bayrob members who had been with the group since its inception, was responsible for hundreds of fraudulent auction postings on eBay, and was the Bayrob member in charge of collecting money from Antonovici and the European money mules. The district court summarily agreed, noting that "there can be more than one leader or organizer of a criminal conspiracy[,]" and after recounting the § 3B1.1(a) factors, stating, "I do, in fact, agree that Mr. Miclaus was, in fact, a leader or organizer, not the sole, but a leader or organizer." R. 230, PID. 3296.

Miclaus did not write code or set up physical or cyber infrastructure for the group, and he received only 10% of the group's profits—the smallest share of any of the Bayrob members.

While these factors would seem to cut against a finding that Miclaus was a leader of the Bayrob group, the § 3B1.1(a) enhancement was for the money-laundering conspiracy specifically, and Miclaus had an outsized role in the group's money-laundering activities: he was the group's most prolific poster on eBay—more than 947 fraudulent auctions—which generated the money that was the raison d'etre of the money-laundering conspiracy, he recruited Antonovici to return to the conspiracy after a multi-year absence, and he exercised control over Antonovici and the other European money mules in his role as the Bayrob member responsible for collecting the profits from the cryptomining scheme and the eBay fraud as they came in from the United States. Miclaus and Nicolescu were also the only two constant members of the conspiracy, as other members came and went over the years Bayrob operated. We must review the district court's decision to apply a leadership-role enhancement under § 3B1.1 deferentially, *Sexton*, 894 F.3d at 794, and on this record, we cannot conclude that the district court committed reversible error in applying a four-level leadership-role enhancement to Miclaus's Guidelines calculation.

D.

The district court imposed a two-level enhancement under U.S.S.G. § 2B1.1(b)(11)(B)(i), which applies "[i]f the offense involved . . . the production or trafficking of any . . . unauthorized access device." Here, the district court concluded that Bayrob's sale of stolen credit-card numbers constituted trafficking in unauthorized access devices. *See* U.S.S.G § 2B1.1 cmt. n.10 (defining "unauthorized access device" as "any card . . . that can be used . . . to obtain money, goods, services, or any other thing of value" that has been "stolen . . . with intent to defraud"). Nicolescu and Miclaus don't dispute that point. Instead, they say that Application Note 2 to U.S.S.G. § 2B1.6 precludes the trafficking enhancement. That provision relates to their aggravated identity theft convictions under 18 U.S.C. § 1028A.

The aggravated-identity-theft statute mandates a two-year sentence if, during the commission of certain enumerated felonies, the defendant "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person[.]" 18 U.S.C. § 1028A(a)(1). A sentence under § 1028A must be served consecutively to any other sentence imposed (except for another § 1028A sentence imposed at the same time). *Id.* § 1028A(b)(2), (b)(4). For that reason, Application Note 2 to U.S.S.G. § 2B1.6 provides:

> If a sentence [for aggravated identity theft] is imposed in conjunction with a sentence for an underlying offense, do not apply any specific offense characteristic for the *transfer, possession, or use* of a means of identification when determining the sentence for the underlying offense. A sentence [for aggravated identity theft] accounts for this factor for the underlying offense of conviction, including any such enhancement that would apply based on conduct for which the defendant is accountable under § 1B1.3 (Relevant Conduct).

U.S.S.G. § 2B1.6 cmt. n.2 (emphasis added). Because the mandatory two-year § 1028A sentence already accounts for "the transfer, possession, or use of a means of identification" during the commission of the predicate offense, Application Note 2 was added "to prevent a defendant from being doubly penalized for the same conduct." *See United States v. Taylor*, 818 F.3d 671, 675 (11th Cir. 2016). Nicolescu and Miclaus read Application Note 2 to say that the mandatory § 1028A sentence already accounts for unauthorized-access-device *trafficking*. Accordingly, they argue, the district court wrongly enhanced their total sentences twice for the same conduct.

The district court reasoned that, despite the mandatory two-year sentence under § 1028A, it could apply a two-level enhancement under § 2B1.1(b)(11)(B)(i) because "trafficking" includes additional conduct not captured in "transfer, possession, or use." R. 230, PID. 3268. We have not yet opined on whether "transfer[ring] . . . a means of identification" as contemplated in § 1028A and Application Note 2 to § 2B1.6 is synonymous with "trafficking [an] unauthorized access device" as used in § 2B1.1(b)(11)(B)(i). If "transferring" and "trafficking" are indeed synonymous, then an enhancement under § 2B1.1(b)(11)(B)(i) would not be appropriate.[5] But if the culpable conduct involved in "trafficking" is "different than or in addition to" the "transfer, possession, or use," then the enhancement can apply. *See Taylor*, 818 F.3d at 675. For example, in *United States v. Lyles*, we rejected a defendant's argument that Application Note 2 prevented a loss-based enhancement under U.S.S.G. § 2B1.1(b)(1). 506 F. App'x 440, 446–47 (6th Cir. 2012). We explained that the loss-based enhancement "punishe[d]

[5]The phrase "means of identification" includes "unauthorized access devices." *See* 18 U.S.C. §§ 1028(d)(7)(D), 1029(e)(3); U.S.S.G §§ 2B1.1 cmt. n.10(A), 2B1.6 cmt. n.2. Therefore, these terms do not create a meaningful distinction between the conduct covered in § 2B1.1(b)(11)(B)(i) and that covered in Application Note 2 to § 2B1.6.

the defendant for inflicting a particular monetary harm rather than for transferring, possessing, or using a means of identification." *Id.* at 447.

Neither § 2B1.1(b)(11), § 2B1.6, nor the relevant commentary defines "traffic" or "transfer."[6] When the Guidelines "do[] not define a term, we generally give the term its ordinary meaning." *Riccardi*, 989 F.3d at 486 (citation omitted). The ordinary meaning of "traffic" carries a commercial aspect, which the word "transfer" does not. *Compare* "Traffic," Oxford English Dictionary, oed.com ("To engage in trade or commerce, esp[ecially] between one country, region, or community and another; to buy and sell, or barter, goods or commodities; to trade."), *and* "Traffic," Am. Heritage Coll. Dict. (3d ed. 1993) ("The commercial exchange of goods; trade."), *with* "Transfer," Oxford English Dictionary, oed.com ("To convey or take from one place, person, etc. to another; to transmit, transport; to give or hand over from one to another."), *and* "Transfer," Am. Heritage Coll. Dict. (3d ed. 1993) ("To convey or cause to pass from one place, person, or thing to another."). As Nicolescu's counsel conceded at oral argument, trafficking is transfer *plus* something else, such as marketing or sale. So, although all "trafficking" involves "transfer," the converse is not true. Here, in addition to "transferring" stolen credit-card numbers to others on the internet, Bayrob also marketed them on AlphaBay and accepted payment in return for their sale. The commercial aspect of "trafficking" is not captured by the § 1028A conviction, and the best reading of the Guidelines suggests that "trafficking" unauthorized access devices should bear additional consequences that mere transfer does not.

By contrast, a Guideline provision adjacent to § 2B1.1(b)(11)(B) illustrates the type of enhancement that § 2B1.6 does prevent. That provision is § 2B1.1(b)(11)(C). It imposes a two-level enhancement for "(i) the unauthorized *transfer* or *use* of any means of identification

[6]Our dissenting colleague points out that one statute defines "traffic" to mean "*transfer*, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of." 18 U.S.C. § 1029(e)(5) (emphasis added). But another nearby statute defines "traffic" to include a commercial component: "[T]he term 'traffic' means . . . (A) to transport, transfer, or otherwise dispose of, to another, *as consideration for anything of value*; or (B) to make or obtain control of with intent to *so* transport, transfer, or otherwise dispose of." *Id.* § 1028(d)(12) (emphasis added). In any event, the relevant Guidelines and Application Notes define many *other* terms using definitions contained in 18 U.S.C. §§ 1028 and 1029. But the Sentencing Commission has not chosen to do so with respect to the word "traffic." Therefore, these statutes are not binding, and we instead look to the ordinary meaning of the disputed terms. *See Riccardi*, 989 F.3d at 486.

unlawfully to produce or obtain any other means of identification, or (ii) the *possession* of 5 or more means of identification that unlawfully were produced from, or obtained by the use of, another means of identification." U.S.S.G. § 2B1.1(b)(11)(C) (emphasis added). Both § 2B1.1(b)(11)(C) and § 2B1.6 use the terms "transfer," "possession," and "use." Section 2B1.1(b)(11)(B) does not; it uses "trafficking." Courts "usually 'presume differences in language like this convey differences in meaning.'" *Wis. Central Ltd. v. United States*, 138 S. Ct. 2067, 2071 (2019) (quoting *Henson v. Santander Consumer USA Inc.*, 137 S. Ct. 1178, 1723 (2017)); *see DePierre v. United States*, 564 U.S. 70, 83 (2011) ("[T]he usual rule [is] that 'when the legislature uses certain language in one part of the statute and different language in another, the court assumes different meanings were intended.'" (quoting *Sosa v. Alvarez-Machain*, 542 U.S. 692, 711 n.9 (2004))); *cf. United States v. Howse*, 478 F.3d 729, 733 (6th Cir. 2007) (finding that identical language in two Guidelines provisions carried the same meaning in each). Because nothing in the Guidelines or commentary suggests that this presumption should not hold, Application Note 2 bars enhancements under § 2B1.1(b)(11)(C) but not "trafficking" enhancements under § 2B1.1(b)(11)(B).

Additionally, treating "trafficking" and "transferring" as equivalent in this context, might render superfluous parts of a related statute, 18 U.S.C. § 1028. "A statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant." *Hibbs v. Winn*, 542 U.S. 88, 101 (2004) (citation omitted). Section 1028 makes it a crime to "knowingly traffic[] in . . . authentication features for use in false identification documents, document-making implements, or means of identification." 18 U.S.C. § 1028(a)(8). But it also, separately, makes it a crime to "knowingly . . . transfer[] . . . a document-making implement or authentication feature . . . [to create] a false identification document." *Id.* § 1028(a)(5). If "transferring" and "trafficking" are the same, these provisions would be redundant.

We acknowledge that our holding charts a new course among our sister circuits, which have held that the trafficking enhancement cannot apply to a defendant convicted of aggravated identity theft. The First Circuit offered the earliest decision on point, reasoning that because the "trafficking of a means of identification *involve[s]* a transfer," it would violate Application Note

2 of § 2B1.6 to impose a trafficking enhancement in these circumstances. *United States v. Jones*, 551 F.3d 19, 25 (1st Cir. 2008) (emphasis added). Other circuits have followed the First Circuit's reasoning. *See United States v. Charles*, 757 F.3d 1222, 1226 (11th Cir. 2014); *United States v. Doss*, 741 F.3d 763, 768 (7th Cir. 2013); *United States v. Lyons*, 556 F.3d 703, 708 (8th Cir. 2009) ("Given that the plain meaning of trafficking *involves* a transfer, the enhancement in § 2B1.1(b)(10)(B)(i) for trafficking of an unauthorized access device is one such specific offense characteristic that cannot be applied." (emphasis added)).

But these circuits apply a different rule entirely to another component of the disputed Guideline. In addition to covering the "trafficking" of an unauthorized access device, § 2B1.1(b)(11)(B) also applies to the "production" of such a device. "Production" would seem to "involve" the "possession" (and potentially also the "use" or "transfer") of an unauthorized access device. Yet, no circuit has held that § 2B1.6 or Application Note 2 can prevent a "production" enhancement. *See Taylor*, 818 F.3d at 676 (upholding an enhancement under § 2B1.1(b)(11)(B)(i) for "production of an unauthorized access device/means of identification [because 'production'] is separate and distinguishable from the mere transfer, possession, or use of such device"); *United States v. Jones*, 792 F.3d 831, 835 (7th Cir. 2015) (same); *United States v. Jenkins-Watts*, 574 F.3d 950, 962 (8th Cir. 2009) (same). And, in an unpublished opinion, so have we. *United States v. Wiley*, 407 F. App'x 938, 942–43 (6th Cir. 2011).

Examining these "production" cases, the proper rule becomes clear: "[I]f the defendant's underlying conduct is limited to transfer, possession, or use of a means of identification of another, then the enhancement cannot apply; if the conduct is different than or in addition to such transfer, possession, or use, then the enhancement can apply."[7] *Taylor*, 818 F.3d at 675. As discussed above, the ordinary meaning of "trafficking" is not "limited to transfer, possession, or

[7]Our dissenting colleague counters that the "production" cases are different because to "produce" is defined in 18 U.S.C. § 1029(e)(4) as to "design, alter, authenticate, duplicate, or assemble." We again question the reliance of a definition outside of § 1028a, *see supra* note 7; but we acknowledge that the Application Notes to § 2B1.1 define "production" similarly, to "include[] manufacture, design, alteration, authentication, duplication, or assembly," § 2B1.1 cmt. n.10. Under this definition, a person engaged in "production" will in most instances also possess or use an unauthorized access device. But that just confirms the point we make here—that the enhancement under § 2B1.1(b)(11)(B) applies when a person does something different than, or in addition to, the transfer, possession, or use of an unauthorized access device.

use." It involves marketing or sales activity beyond mere "transfer"—it is transfer plus something more.

Bayrob's marketing and sales of stolen credit cards constituted trafficking in unauthorized access devices. Accordingly, the district court did not err in adding a two-level enhancement under § 2B1.1(b)(11)(B)(i).

Perhaps seeing the writing on the wall, Miclaus hedges his argument. He contends that even if the stolen-credit-card sales fall under the trafficking enhancement, the enhancement still should not apply to him. In support, Miclaus points out that he did not sell the credit cards himself. He also thinks the credit card sales fell outside the scope of Bayrob's jointly undertaken criminal activity, meaning he cannot be held liable for the acts of his credit-card-trafficking codefendants. *See* U.S.S.G. § 1B1.3(a)(1)(B)(i)-(iii) (stating that, under the Sentencing Guidelines, a defendant may be liable for acts of others that were "(1) within the scope of the jointly undertaken criminal activity, (2) in furtherance of that criminal activity, and (3) reasonably foreseeable in connection with that criminal activity").

Because Miclaus did not object to the application of the trafficking enhancement at the sentencing hearing, we review his challenge for plain error. *See United States v. Vonner*, 516 F.3d 382, 385 (6th Cir. 2008) (en banc).

The district court did not err, much less plainly. The record shows Bayrob sold the stolen credit cards on AlphaBay, a website on the dark web, from 2014 to 2016. With prices for the cards ranging from $1 to $35, Bayrob's AlphaBay profile boasted 500 transactions, representing between 1,000 and 2,000 credit card sales. Although Miclaus may not have managed these AlphaBay transactions directly, he did receive the profits. At trial, his codefendant testified that he delivered the cash proceeds of the credit card sales straight to Miclaus.

This testimony rebuts Miclaus's first point. He may not have sold the cards himself, but his role in collecting the proceeds shows he played a part in the trafficking scheme. Miclaus's second point, about the scope of Bayrob's jointly undertaken criminal activity, falls with his first. Trial testimony showed at least five Bayrob members, including Miclaus, helped traffic the stolen credit cards on AlphaBay. We consider the number of credit card sales, the number of

Bayrob members directly involved, and the two years of sales on AlphaBay together. In light of this evidence, Miclaus cannot plausibly claim the stolen credit card sales fell outside the scope of Bayrob's jointly undertaken criminal activity. And, as a result, we reject Miclaus's separate argument. The district court did not err in applying the trafficking enhancement to Miclaus.

E.

The district court applied a four-level enhancement under U.S.S.G. § 2B1.1(b)(19)(A)(ii), which applies when a defendant is convicted of an offense under § 1030(a)(5)(A). Miclaus and Nicolescu were convicted on Count 14, which alleged a § 1030(a)(5)(A) violation as one of the objects of a conspiracy under 18 U.S.C. § 371, but they were convicted of the § 371 conspiracy—not a substantive offense under § 1030(a)(5)(A). The government concedes error, and we agree.[8] The district court erred in applying a four-level enhancement under § 2B1.1(b)(19)(A)(ii) because Nicolescu and Miclaus were not convicted of an offense under § 1030(a)(5)(A).

IV.

The district court determined that after all the sentencing enhancements were applied, Nicolescu and Miclaus had an adjusted offense level of forty-three. The parties then agreed to subtract an additional five levels, down to an offense level of thirty-eight, which yielded a Guidelines range of 235 to 293 months' imprisonment.

The district court's errors in imposing a two-level enhancement under § 2B1.1(b)(4) for receiving and selling stolen property, and a four-level enhancement under § 2B1.1(b)(19)(A)(ii) for being convicted of an offense under § 1030(a)(5)(A) resulted in six levels being erroneously added to Nicolescu's and Miclaus's offense level. At thirty-seven, the correct level, their category I criminal history yields a Guidelines range of 210 to 262 months' imprisonment. Though the district court sentenced Nicolescu and Miclaus below the incorrectly calculated range on Counts 1 through 13 and 21, and their sentences for those counts fall within (Nicolescu) and below (Miclaus) the correctly calculated range, we cannot conclude that the errors were

[8]Only Miclaus objected to this enhancement, but the government agreed to forego an abandonment argument with respect to Nicolescu.

harmless.[9] "[B]ecause the Guidelines range is the starting point for the district court's analysis[,]" and absent some indication that the district court would have imposed the same sentence regardless of the error, it is for the district court to "decide whether, starting from the correct Guidelines range, a downward variance remains appropriate." *United States v. Montgomery*, 998 F.3d 693, 700 (6th Cir. 2021). Accordingly, we remand so that Nicolescu and Miclaus can be resentenced under a correctly calculated Guidelines range.

V.

For the reasons set forth above, we **AFFIRM** Nicolescu's and Miclaus's convictions, **VACATE** their sentences, and **REMAND** for resentencing.

[9]Miclaus failed to object to the § 2B1.1(b)(4) enhancement below, so our review with respect to Miclaus is for plain error. But even under plain-error review, Miclaus is entitled to resentencing under a correctly calculated Guidelines range because the error was clear, it affected his substantial rights, and it affected the fairness of the proceedings below. *See Rosales-Mireles v. United States*, 138 S. Ct. 1897, 1907–08, 1911 (2018); *Molina-Martinez v. United States*, 136 S. Ct. 1338, 1343 (2016).

DISSENT

HELENE N. WHITE, Circuit Judge, concurring in part and dissenting in part.

I would not affirm the imposition of the two-level enhancement under U.S.S.G. § 2B1.1(b)(11)(B)(i) for "trafficking" in unauthorized access devices.

The district court applied the two-level enhancement to the grouping that included the wire-fraud convictions because the relevant conduct included Bayrob's sale of stolen credit-card information on AlphaBay, and the district court found that this conduct constituted "trafficking" in unauthorized access devices for purposes of § 2B1.1(b)(11)(B)(i). I do not quarrel with that aspect of the analysis. The problem with applying an enhancement under § 2B1.1(b)(11)(B)(i) for "trafficking" in this case is that Defendants were also convicted of § 1028A aggravated identity theft, and another provision of the Guidelines, Application Note 2 to U.S.S.G. § 2B1.6, precludes any enhancement to the underlying offense (here, wire fraud) "for the transfer, possession, or use" of a means of identification (the stolen credit-card information) when a defendant is already subject to a mandatory two-year consecutive sentence under § 1028A for the "transfer, possession, or use" of a means of identification. The application note recognizes that allowing both would impermissibly punish the defendant twice for the same conduct. *United States v. Taylor*, 818 F.3d 671, 675 (11th Cir. 2016).

"Trafficking" a stolen credit-card number necessarily involves transferring it. Neither § 2B1.1(b)(11)(B)(i) nor § 2B1.6 define "trafficking." But 18 U.S.C. § 1029 (the very next provision of the United States Code after § 1028A) which prohibits "traffic[king] in . . . unauthorized access devices," defines "traffic" to mean "*transfer*, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of[.]" § 1029(e)(5) (emphasis added). Thus, in enhancing Defendants' sentences for "trafficking" stolen credit-card numbers, the district court also impermissibly punished them a second time for the inextricable element of "transferring" them, which is expressly prohibited by Application Note 2 of § 2B1.6.

That is why every court of appeals to consider the issue has held that the § 2B1.1(b)(11)(B)(i) "trafficking" enhancement cannot be imposed in these circumstances. *See United States v. Lyons*, 556 F.3d 703, 708 (8th Cir. 2009) ("Given that the plain meaning of trafficking involves a transfer, the enhancement in § 2B1.1(b)([11])(B)(i) for trafficking of an unauthorized access device is one such specific offense characteristic that cannot be applied" because of Application Note 2 to § 2B1.6); *United States v. Jones*, 551 F.3d 19, 25 (1st Cir. 2008) (holding that § 2B1.1(b)(11)(B)(i) enhancement was precluded by Application Note 2 to § 2B1.6 because under "the plain meaning of the words, [the defendant's] trafficking of a means of identification involved a transfer (though the reverse is not necessarily true)"); *United States v. Charles*, 757 F.3d 1222, 1226–27 (11th Cir. 2014) (same); *United States v. Doss*, 741 F.3d 763, 766–68 (7th Cir. 2013) (same).

Lastly, the majority's invocation of cases permitting an enhancement under the "production" prong of § 2B1.1(b)(11)(B) is unavailing. The majority reasons that "'[p]roduction' would seem to 'involve' the 'possession' (and potentially also the 'use' or 'transfer') of an unauthorized access device," and so if we recognize production as a distinct action supporting the enhancement, we should likewise permit an enhancement for trafficking when "the [punished] conduct is different than or in addition to such transfer, possession, or use." Maj. Op. at 31. However, unlike trafficking, production is statutorily defined as different in kind from "transfer, possession, or use." While 18 U.S.C. § 1029's definition of "traffic" includes the word "transfer," its definition of "produce" does not similarly include any aspect of the § 1028A "transfer, possession, or use" language, defining it instead to include "design, alter, authenticate, duplicate, or assemble." § 1029(e)(4)-(5).

Accordingly, I dissent from the affirmance of the application of the § 2B1.1(b)(11)(B)(i) enhancement.